# Stopping Fraud: Detecting and Preventing Fraud in the e-Health Era



By Lisa A. Eramo

---

*Stopping fraud will require health record systems, organizations, and individuals capable of, and committed to, detecting and preventing false claims before they are paid.*

---

Healthcare fraud continues to plague the country, costing the United States billions of dollars per year.

The most frightening part? Much of it goes completely under the radar, says William J. Rudman, PhD, a coauthor of a November 2010 report that explores the prevalence of fraud and its implications for HIM professionals. The study, conducted by the AHIMA Foundation, found that very few cases of fraud are even detected. Those that are detected only surface after years of aberrant data patterns raise a red flag.

"We are probably only at the tip of the iceberg in terms of being able to identify and understand fraud," Rudman says. "In big corporations, it may take four or five years to document cases of fraud. Even in physician offices, it takes a lot of time and manpower to identify and address it."

Yet despite the difficulty in detecting it, one thing is very clear. "Healthcare fraud is the most lucrative thing you can do if you're a crook. It's massive," says Donald W. Simborg, MD, independent health IT consultant in Nevada City, CA.

Stopping fraud will require health record systems, organizations, and individuals capable of, and committed to, detecting and preventing false claims before they are paid.

## Billions Paid in False Claims

Financial fraud and false claims are the most common types of healthcare fraud, according to the AHIMA Foundation report. This includes false claims for medically unnecessary services; false claims that include purposeful overstatement of the amount, number, type, or complexity of the service provided; or false claims that include services that were never rendered or were not rendered on the individuals claimed or by the provider claimed.

The steadily growing problem of healthcare fraud has attracted attention at the federal level. The Obama administration allocated a $1.7 billion increase over five years to support the Health Care Fraud and Abuse Control program, which is designed to coordinate federal, state, and local law enforcement activities. The Healthcare Fraud Prevention and Enforcement Action Team, a combined effort of the Departments of Justice and Health and Human Services announced in May 2009, will also address fraud and abuse.

Will this increased federal focus help reduce the number of fraudulent cases? Not quite, says Simborg. Although the intent may be there, the government's reactive-rather than proactive-approach to detecting fraud and abuse simply won't work, he says.

"What we do now is pay and chase. You pay the bill and then do a pattern analysis to find outliers. Then you do a sting operation to recover maybe a million or billion dollars," he says. "This is a drop in the bucket. We're talking about a $250 billion problem."

Rudman agrees. Healthcare fraud and abuse may persist-and even worsen-as hospitals and providers continue to adopt electronic health records (EHRs), he says. "As technology changes, those who intend to commit fraud are always going to be

one step ahead of those who are trying to detect it."

That's because EHRs make it easy for thieves to fabricate information. For example, providers can easily produce fraudulent yet credible claims by creating virtual episodes of care that fly completely under an insurer's radar, Simborg says. Identity theft of both patients and providers is also a likely possibility. These are just two examples of how easy it is to commit fraud in an electronic environment-all with the simple click of a mouse, he says.

## Detecting False Claims before They Are Paid

Stopping fraudulent claims before they are paid will require individuals and organizations committed to preventing fraud and EHR systems that are capable of detecting it.

Fraud and abuse fall under an HIM professional's purview, says Rudman, a former educator and current vice president of education and workforce at AHIMA. "HIM professionals take an oath to ensure data integrity and the authenticity of data. Their job is to ensure that everything in the record is timely and accurate."

HIM professionals are also skilled in the areas of data management and manipulation-both of which play an important role in fraud detection and tracing aberrant data patterns over time, Rudman says. In addition, HIM professionals have extensive training in the privacy and security of the medical record, computer technology, and audit trail analysis, he adds.

"They are the only profession within the hospital that has training in both clinical outcomes/processes and information technology," he says.

They are also the ones who can advocate for embedding fraud prevention and detection features directly into EHRs and other health IT, says Simborg. If EHRs do not begin to incorporate fraud management, fraud and abuse will only continue to rise. Hospitals need to use health IT-specifically EHRs-at the point of care to prevent fraud before it occurs, he adds.

"If we can do better authentication at the point of care to ensure that a real person and a real doctor got together for a visit, this would help so much," says Simborg. "It would practically eliminate all the fraud that's happening when people are fabricating visits, which is a big part of fraud."

For example, hospitals can use biometrics such as thumb prints or iris scans at the point of care to verify the patient's identity. Not only would this simplify the registration process, it would also help prevent identity theft.

### Demonstrating Services Were Rendered

Another solution is to integrate highly detailed-and standardized-audit trails into EHRs that would help detect fraud. Hospitals should be required to send an audit log with each claim so the Centers for Medicare and Medicaid Services can examine the logs electronically before paying the bills.

These audit trails, which would include a date and time stamp for each clinical entry and essentially any other access to the EHR, would be particularly helpful in terms of preventing fraud related to the high-risk area of E/M coding, Simborg says.

The ability to produce a complete history and physical with a "simple click and not doing any of the work" is highly problematic, he says. Canned notes also make it easy for physicians to fabricate a level IV or V visit that should have only been coded as a level I or II. "If an audit trail reveals that the physician did all of this with one click for every visit, you'd know you've got a fraudulent physician," he says.

Simborg also believes that audit trails and other functionality aimed at enhancing fraud management should be a part of the EHR certification process. In 2007 Simborg led an expert panel convened by the Office of the National Coordinator for Health IT that recommended 14 fraud prevention and detection functions that should be required of all EHRs. One suggested function is a traceable and auditable path from a claim payment or a transmission of a pay-for-performance payment to the clinical documentation supporting it.

Other examples include proxy authorship (i.e., retaining the date/time/user stamp of the individual who originally entered the data as well as the individual entering data on behalf of someone else), read-only access (e.g., for EHR auditors), and the

ability to document that staff members completed identity proofing as well as the method used to verify the patient's identity (e.g., a photo ID check).

"These are very simple measures that would eliminate huge amounts of fraud or make it very easy to detect," Simborg says. "The return on investment for this work is enormous."

**Requiring Fraud Detection Functionality**

To date, federal meaningful use requirements do not include a fraud prevention component, and EHR certification related to the program thus does not require it.

This lack of emphasis on fraud detection may be due to the fact that fraud management can potentially be a barrier to physician adoption of EHRs, Simborg says.

"HIM professionals are trying their best to get physicians to adopt EHRs, but physicians are very paranoid of being accused of fraud," he says. "There are a lot of legitimate complaints. If they get accused of Medicare fraud, it can cost $100,000 or $200,000 to defend themselves."

The solution to this resistance may be better documentation improvement efforts and physician education that help alleviate fears and make physicians more confident in their billing and documentation practices, Simborg suggests.

Requiring EHR vendors to incorporate fraud management as part of the certification process will also help HIM professionals advocate for change, according to Simborg. "HIM professionals are in a very difficult position. They don't have anyone backing them outside the organization like CMS, the [Office of the Inspector General], and the ONC," he says. "They don't want to become adversaries of their own providers."

Aside from the EHR, other technologies may be helpful in detecting and preventing fraud as well. For example, computer-assisted coding can detect coding errors and fraudulent practices over time, Rudman notes. It also includes real-time prompts and decision support tools that help justify claims based on physician documentation. "If it's not documented, it's very difficult to upcode. It can provide a nice check and balance," he says.

HIM professionals can advocate for fraud detection and prevention within their facilities or on a national level in many other ways, say Rudman and Simborg. They can:

- Stay up-to-date on new regulations and laws pertaining to fraud and abuse
- Advocate for the adoption of computer-assisted coding technology in their hospitals
- Participate in leadership roles on fraud and abuse committees and initiatives
- Stay actively involved in national and local policy decisions related to fraud and abuse prevention and detection
- Educate consumers about medical identity theft and safeguarding their health information

## Winter *Perspectives* Shares Health IT Stories from Underserved Communities
**http://perspectives.ahima.org**

The Winter 2011 issue of *Perspectives in Health Information Management* features stories from healthcare providers in medically underserved communities sharing their health IT successes and failures.

The issue was co-edited by Commander David A. Dietz, MSW, MHSA, and Garth N. Graham, MD, MPH, of the Office of Minority Health of the Department of Health and Human Services. Papers in the issue include the following:

- "A Patient-Centric, Provider-Assisted Diabetes Telehealth Self-management Intervention for Urban Minorities" examines the implementation of an urban diabetes telehealth self-management intervention for a sample of inner-city African Americans with diabetes.
- "A Peach of a Telehealth Program: Georgia Connects Rural Communities to Better Healthcare" reviews the deployment of a statewide telehealth network in Georgia.

- "Innovation in Indian Healthcare: Using Health Information Technology to Achieve Health Equity for American Indian and Alaska Native Populations" provides an overview of efforts to use health IT to achieve health equity for American Indian and Alaska Native communities.
- "Role of Mobile Health in the Care of Culturally and Linguistically Diverse US Populations" reviews public policy with the goal of improving the care of patients belonging to culturally and linguistically diverse populations.
- "Use of Health Information Technology among Racial and Ethnic Underserved Communities" examines the potential role of health IT in addressing healthcare disparities among racial and ethnic minority populations.

Dietz and Graham note that there is no greater time than now to exercise innovation and expertise in response to the ethical imperative that all Americans-regardless of race or ethnicity, income, or age-receive the highest quality of healthcare services possible.

*Perspectives*, a scholarly, peer-reviewed research journal published by the AHIMA Foundation, advances health information management practice and encourages interdisciplinary collaboration between HIM professionals and others in disciplines supporting the advancement of the management of health information.

**Audio Online** **http://journal.ahima.org**
Study coauthor William Rudman speaks about what HIM professionals can do to prevent fraud.

Lisa A. Eramo (leramo@hotmail.com) is a freelance writer and editor in Cranston, RI, who specializes in healthcare.

**Article citation**:
Eramo, Lisa A. "Stopping Fraud: Detecting and Preventing Fraud in the e-Health Era" *Journal of AHIMA* 82, no.3 (March 2011): 28-30.